Standard Operating Procedure

OIT Standard Operating Procedures Forms Index

Document Owner: OIT	Document ID:	
Technical Area: IAM, Server, Database, EA, SecOps, Network, SRC, Desktop/Deskside, OIS, CTO	Effective Date:	
Version: 0.2	Last Reviewed Date:	

Office of Information Technology (OIT) SOP Forms Index

Table of Contents

Purpose:

The purpose of the OIT SOP Forms Index document is to create and maintain **audit requirements documentation**, in support of processes, procedures, and standards of Infrastructure Operations and application data flow.

Cyber Pol 102 - Access Control

SOP Purpose: Standard operating procedure for identifying specific Governor's Office of Information Technology (OIT) requirements for Cyber Pol 102 Access Control, that details; Account Management, Least Privilege, and Remote Access. For a copy of related SOPs for specific agencies, please reach out to the Identity & Access Management (IAM) team.

Scope:
These requirements apply to the Identity & Access Management, Server, Database and SecOps teams.

Requirements:

- **8.1 Account Management**
    - Additional Notes:
        - While the data is owned by the Agency, the agency must direct the ultimate requirements around this management, though they work in collaboration with OIT.
        - Each state agency has their own Access Request Form. The Colorado Department of Transportation (CDOT) has their own VPN Access Request Form.
        - The OIT Access Request Form requires an authorized person to provide two signatures. Only one signature is required for CDOT VPN-Only Access Request Form. Authorized signatures are typically a supervisor or manager of the person for which the access is requested. If there is not a designee, please ask your manager.
        - Agencies must notify OIT to offboard/deprovision accounts under the OIT account management. For a copy of related SOPs for specific agencies, please reach out to the IAM team.
        - <u>Higher Level Account Management:</u> If the identified business function includes data with additional compliance requirements, such as Federal Tax Information (FTI), Social Security Administration (SSA), Criminal Justice Information (CJI), etc., then the IAM provisioning must additionally confirm that the prerequisites to access are provided prior to, or within the required timeline.
        - No input/resource from the Applications team provided.
- **8.5 Least Privilege**
    - See below *Attachments/Folder*: *Least Privileged Access* link.

- **8.12 Remote Access**
    - See below *Attachments/Folder: Remote Access to State Network* link.

Attachments/Folder:

- AC - Access Control CYBER POL 102
- CISP-001 Access Control
- OIT Access Request Forms
- Security Access Request Process
- *Remote Access to State Network*
- Least Privileged Access
- Server Administrator Offboarding SOP
- Database Software Management
- Database Security Policy
- Identity and Access Administration
- NIST SP 800-53 rev 4 (or as amended), AC family

Cyber Pol 108 - Identification and Authentication

SOP Purpose: Standard operating procedure for identifying specific Governor's Office of Information Technology (OIT) requirements for Cyber Pol 108 Identification and Authentication, that details; Identification and Authentication (Users and Devices), Identifier Management, and Authenticator Management. For a copy of related SOPs for specific agencies, please reach out to the Identity & Access Management (IAM) team.

Scope:
This requirement applies to the Identity & Access Management team.

Requirements:

- 8.1 Identification and Authentication (Users and Devices)
- 8.2 Identifier Management
- 8.3 Authenticator Management
    - Additional Note:
        - Applications used by state workers require a sign on with a username and password. Access is not permitted to applications without logging on to the network, and some applications require an additional sign on. **Note**: For some applications, like Microsoft Word, or Sticky Notes, they do not require a login to use.

Attachments/Folder:

- Identification & Authentication Cyber Pol 108
- Remote Access to State Network SOP
- CISP-007 Identification and Authentication
- Security OIT Password Standards
- Server Administrator Offboarding SOP
- Secure Configuration Exception Request SOP
- Database Security Policy

Cyber Pol 113 - Personnel Security Policy

SOP Purpose - Standard operating procedure for identifying specific Governor's Office of Information Technology (OIT) requirements for Cyber Pol 113 Personnel Security, that details; Personnel Termination, Personnel Transfer, and Third-Party Security. For related SOPs for specific agencies, please reach out to the Identity & Access Management (IAM) team.

Scope: These requirements apply to the Identity & Access Management and HR team and HR.

Requirements

- **8.3 Personnel Termination**
    - Additional Notes:
        - It is the responsibility of each agency to inform IAM when an employee goes through the process of offboarding.
- **8.4 Personnel Transfer**
    - Additional Notes:
        - When an employee transfers from one agency to another, the employee is fully deprovisioned from OIT, then provisioned to the new agency.
        - OIT will suspend and change the existing email address for the transferring employee. The email address will be restarted as the same address on the back end, but it will be a new email address for the transferring employee.
- **8.6 Third-Party Security**
    - HR - HR does not have a Third-Party Security SOP in place at this time.

Attachments/Folder:

- PS - Personnel Security Cyber Pol 113
- AC - Access Control CYBER POL 102
- *Security Access Request Process*
- CISP-012 Personnel Security
- NIST SP 800-53 rev 4 (or as amended),Family

Cyber Pol 106 - CM Configuration Management

SOP Purpose: Standard operating procedure for identifying specific Governor's Office of Information Technology (OIT) requirements for Cyber Pol 106 Configuration Management, that details; Configuration Settings and Information System Component Inventory. For related processes for specific agencies, please reach out to the Network and Server team.

Scope:
These requirements apply to the Server, Network, Database, Deskside, SecOps and Applications teams.

Requirements:

- **8.5 Configuration Settings**
  - Additional Notes:
    - 8.5.1 - OIT shall establish and document secure configuration settings for information technology products (e.g., mainframe computer, servers, workstations and other network components as well as database, operating systems and applications) employed within the information system using the Center for Internet Security (CIS) Hardening Guidelines as a standard.
    - Database Services retains policies, standards and SOPs for Oracle and SQL server environments. **Note**: The old environment is to be decommissioned (date to be determined).
    - Policies are the overall high-level policies that govern how Database Services operates. Standards document what Database Services ensures, and SOPs provide more detailed how-to steps for each standard.
  - Additional Notes:
    - There are many potential different device configuration parameters, and configuration settings vary widely based on the different device platforms.
    - The Server teams use Microsoft Server Configuration best practices and CIS hardening guidelines for configuration settings on the servers themselves. Specific configuration on each server can be dependent on the applications and functions the server is being used for.
    - Network uses SolarWinds Orion Server with various modules like Network Performance Monitoring (NPM) and Network Configuration Management (NCM) for active network device inventory and monitoring. Not all agencies have NCM. Colorado Department of Labor and Employment (CDLE) does not have the NCM Module Licensing in SolarWinds.
    - No input/resource from the Applications team.
- **8.7 Information System Component Inventory**
  - Pending SOP process development - ITAM:

- For sections 8.7.1, 8.7.3, and 8.7.4, OIT has never had an ITAM repository, the IT Asset Management (ITAM) team is building processes and documentation from the ground up. **Note**: As of 12/3/2019, there are no specifics on a timeline. ITAM is in the process of proposing timelines to IT Steering, and there are a lot of moving cogs right now (Senate Bill/Gov's Office/Legislation & Committees, implementing new processes for asset intake, possibility of an ITSM, etc.), but it is in progress.
- 8.7.1 & 8.7.4, which also combines into section 8.8, the goal is to utilize a Configuration Management Database (CMDB), but it's a work in progress as well since most CMDB's need ITAM setup first.
- 8.7.2 Network Scanning is in place and there are several tools implemented (not connected to an ITAM repository). The primary tool is System Center Configuration Management (SCCM) for Windows based devices. There are other tools like Splunk, Solarwinds, etc.
- Server team - Data is contained spreadsheets, there is not a consistent methodology for keeping it updated across all of the agencies.

Attachments/Folder:

- CM - Configuration Management Cyber Pol 106
- CISP-005 Configuration Management
- NIST SP 800-53 rev 4 (or as amended), Family
- Database Services Technical Policies
- DBMS Server Inventory Standard
- Security Architecture SOP
- CIS Hardening Standards and Guidelines
- Secure Configuration Exception Request SOP
- Endpoint Configuration Policy (Deskside)

Cyber Pol 114 - Risk Assessment

SOP Purpose: Standard operating procedure for identifying specific Governor's Office of Information Technology (OIT) requirements for Cyber Pol 114 Risk Assessment, that details; Security Categorization, Risk Assessment, and Vulnerability Scanning.

Scope:
These requirements apply to the Server, Network, Database, Deskside, SecOps and SRC teams.

Document Owner: OIT	Document ID:	
Technical Area: IAM, Server, Database, EA, SecOps, Network, SRC, Desktop/Deskside, OIS, CTO	Effective Date:	
Version: 0.2	Last Reviewed Date:	

Requirements:

- 8.1 Security Categorization
- 8.2 Risk Assessment
- 8.3 Vulnerability Scanning
    - Additional Notes:
        - SecOps Threat and Vulnerability Management Program (TVMP) is responsible for identifying existing and new vulnerabilities related to those systems and applications operated and/or managed by OIT.
        - Classifies a vulnerability for OIT.
        - Scanning tool knowledge base is updated frequently to identify new vulnerabilities timely so system owners can apply the necessary patches.
        - For the Vulnerability process, SecOps uses a paper form that is submitted to the service desk and sent to SecOps staff to perform work.
        - SecOps is in the process of rolling out a new Vulnerability management program. The team is in the process of developing SOP (completion date TBD).
        - Server team will make sure the software is installed on every server as part of a server deployment.
        - SecOps team will run periodic automated scans on the endpoints. Assigned server team personnel will be notified when a report is available. Refer to *Security Tools SOP*.
        - Covers Information System Monitoring. Refer to section *Cyber Pol 117 System and Information Integrity*.
        - Covers Management Enforcement. Refer to section *Cyber Pol 101 Configuration and Patch Management (Requirement 8.4)*.
        - Covers Continuous Monitoring. Refer to section *Cyber Pol 105 Security Assessment and Authorization*.
        - **Note**: The Security Tools SOP is currently a work in progress. As the corresponding policy is updated, this document will be revisited.

Attachments/Folder:

- RA - Risk Assessment Cyber Pol 114
- CISP-013 Risk Assessment
- NIST SP 800-53 rev 4 (or as amended), Family
- FTI Risk Assessment Procedure
- Audit Remediation Procedure (SRC Team Audit Responsibilities)
- Security Tools SOP
- SRC Team Audit Responsibilities
- The National Institute of Standards and Technology’s National Vulnerability Database (NVD) Common Vulnerability Scoring System version 2 (CVSS V2)

Cyber Pol 105 - Security Assessment and Authorization

SOP Purpose: Standard operating procedure for identifying specific Governor's Office of Information Technology (OIT) requirements for Cyber Pol 105 Security Assessment and Authorization, detailing Continuous Monitoring.

Scope:
This requirement applies to SecOps and SRC teams.

Requirements:

- 8.5 Continuous Monitoring
    - Additional Notes:
        - FTI Risk Assessment Procedure covers the Continuous *Monitoring* section.
        - For Security Operations, refer to Attachments/Folder section,*Audit Logging* link below.

Attachments/Folder:

- CA-Security Assessment and Authorization Cyber Pol 105
- CISP-004 CA Security Assessment and Authorization
- NIST SP 800-53 rev 4 (or as amended), Family
- FTI Risk Assessment Procedure
- Audit Logging

Cyber Pol 117 - System and Information Integrity

SOP Purpose: Standard operating procedure for identifying specific Governor's Office of Information Technology (OIT) requirements for Cyber Pol 117 System and Information Integrity, that details; Information System Monitoring, Security Alerts, Advisories, and Directives, Software, Firmware, and Information Integrity. For related processes for specific agencies, please reach out to the Network and Server team.

Scope:
These requirements apply to the Server, Network, Database, Deskside, SecOps and OIS teams.

Requirements:

- 8.3 Information System Monitoring

    - Additional Notes:
        - There is not any single SOP in place, but for many agencies Network Infrastructure is utilizing Terminal Access Controller Access Control System (TACACS) Plus for the AAA authentication, authorization, and accounting using either Cisco ACS (Access Control Services) or Cisco ISE (Identity Services Engine) appliances to handle the control of administrator access and accounting of logins and configuration changes being made on the network communications devices.
        - Since there are different systems deployed for the AAA systems being used for these purposes, there is not one single SOP.
        - Covers *Cyber Pol 105 Security Assessment and Authorization*
        - Covers Cyber Pol 101 Configuration and Patch Management (Requirement 8.4)
        - Refer to Deskside Services for related SOP.
- 8.4 Security Alerts, Advisories, and Directives
    - Additional Note:
        - Once OIS puts security alerts, advisories, and directives in place, then the person that receives this information will take the necessary action items to resolve the issues.
        - OIT staff will identify which banner and template to use when a notification needs to be sent from the OIT Service Desk.
        - SecOps - Refer to SecOps for related SOP.
- 8.5 Software, Firmware, and Information Integrity
    - Additional Note:
        - Server - refer to Attachments/Folder section, *Notification Procedure* link below.
        - Refer to Deskside Services for related SOP.

Attachments/Folder:

- SI-System and Information Integrity Cyber Pol 117
- CISP-116 System and Information Integrity
- NIST SP 800-53 rev 4 (or as amended), Family
- Notification Procedure

Cyber Pol 101 Configuration and Patch Management

SOP Purpose: Standard operating procedure for identifying specific Governor's Office of Information Technology (OIT) requirements for Cyber Pol 101 Configuration and Patch Management, that details; Baseline Secure Configurations for Servers, Desktops, and Network Devices, Patch Management, and Patch Management Monitoring and Enforcement. For a copy of related SOPs for SecOps Patch Management, please reach out to the SecOps team.

Scope:
These requirements apply to Server, Network, Deskside and SecOps teams.

Requirements:

- 8.1 Baseline Secure Configurations for Servers, Desktops, and Network Devices
  - Additional Note:
    - The Network Services teams use the CIS Hardening Standards and Guidelines. Refer to Attachments/Folder section: *CIS Hardening Standards and Guidlines*.
- 8.2 Patch Management
- 8.4 Patch Management Monitoring and Enforcement
  - Additional Note:
    - 8.4.2 The TVMP will perform monthly automated scans of OIT administered and managed systems for both vulnerabilities and compliance with CIS benchmarks. The automated vulnerability management system will provide role based access for designated users to obtain scan results and prioritized vulnerability solutions. (8.4.2 - Section a removed)
    - All patches should be first deployed and tested in a lower environment before applying to production servers in accordance with the change management process.

Attachments/Folder:

- RA - Risk Assessment Cyber Pol 114
- CISP-005: Configuration Management
- Security Tools
- CIS Hardening Standards and Guidelines
- Configuration & Patch Management Policy - Cyber Pol 101
- NIST SP 800-53 rev 4 (or as amended), Family
- DBMS Patch Management Standards
- Server DBMS Patch Management Procedures
- Endpoint Configuration Policy (Deskside)
- Patch Management Policy (Deskside)

Cyber Pol 104 - Audit and Accountability

SOP Purpose: Standard operating procedure for identifying specific Governor's Office of Information Technology (OIT) requirements for Cyber Pol 104 Audit and Accountability that details; Audit Review, Analysis and Reporting.

Scope: This requirement applies to Server, Network, and Database teams.

Requirements:

- 8.5 Audit Review, Analysis and Reporting

Attachments/Folder:

- AU - Audit & Accountability Cyber Pol 104
- CISP-003: Audit and Accountability
- NIST SP 800-53 rev 4 (or as amended), Family
- Audit Log Review and Monitoring
- Database Security Policy

Cyber Pol 115 - System and Services Acquisition

SOP Purpose: Standard operating procedure for identifying specific Governor's Office of Information Technology (OIT) requirements for Cyber Pol 115 System and Services Acquisition that details; Information System Documentation.

Scope: This requirement applies to the Server, Database and Applications teams.

Requirements:

- 8.4 Information System Documentation
    - Additional Note:
        - No input/resource from the Applications team.

Attachments/Folder:

- SA - System and Services Acquisition Cyber Pol 115
- CSP-115: System and Services Acquisition
- NIST SP 800-53 rev 4 (or as amended), Family
- OIT Database Security Policy
- Security Tools SOP

Cyber Pol 116 - System and Communications Protection

SOP Purpose: Standard operating procedure for identifying specific Governor's Office of Information Technology (OIT) requirements for Cyber Pol 116 System and Communications Protection that details; Boundary Protection, Transmission Confidentiality and Integrity and Protection of Information at Rest.

Scope: These requirements apply to Network, Firewall, Database and Applications teams.

Requirements:

- 8.5 Boundary Protection
    - Additional Note:
        - Enterprise Firewall Design Standard enables an efficient and effective design and implementation of firewalls while providing the desired secure access and data sharing between all business partners.
- 8.6 Transmission Confidentiality and Integrity
    - Additional Note:
        - Communication integrity is typically handled by using Transport Layer Security (TLS), Secure Sockets Layer (SSL), Secure Shell (SSH), or other encryption protocols for communications between servers, or between client and server.
- 8.19 Protection of Information at Rest
    - Additional Note:
        - Data base - Regarding Database Service (DBS) policies; if there is a CIS policy in place that covers Protection of Information at Rest, we simply try to follow that policy, we don't have a separate policy for the same thing.
        - No input/resource from the Applications team.

Attachments/Folder:

- SC - System and Communications Protection Cyber Pol 116
- CISP-115: System and Communications Protection
- NIST SP 800-53 rev 4 (or as amended), Family
- Database Security Policy
- TS-CISO-004_Technical - OIT Standards - Firewall Design Standard v1.1

Cyber Pol 110 - System Maintenance

SOP Purpose: Standard operating procedure for identifying specific Governor's Office of Information Technology (OIT) requirements for Cyber Pol 110 System Maintenance that details; Controlled Maintenance, Maintenance Tools and Non-Local (Remote) Maintenance. For a copy of related SOPs for Deskside Services, please reach out to the Deskside Services team.

Scope: These requirements apply to Network, Server, Database and Deskside Services teams.

Requirements:

- 8.1 Controlled Maintenance
- 8.2 Maintenance Tools
  - Additional Note:
    - The Network & Voice Services does not have an SOP that deals with Hardening.
- 8.3 Non-Local (Remote) Maintenance
  - Additional Note:
    - Network devices, the Network Services Teams use the CIS Hardening Standards and guidelines. Refer to *Attachments/Folder section, CIS Hardening IOS 15 4.0.0 Benchmark OIT NetOps* link.

Attachments/Folder:

- MA - System Maintenance Cyber Pol 110
- NIST SP 800-53 rev 4 (or as amended), Family
- CISP 009: System Maintenance
- Database System Maintenance
- Unsupported System Components
- CIS Hardening IOS 15 4.0.0 Benchmark OIT NetOps

Cyber Pol 118 - Security Planning

SOP Purpose: Standard operating procedure for identifying specific Governor's Office of Information Technology (OIT) requirements for Cyber Pol 118 Security Planning that details; Information System Security Plans (SSP) and Information Security Architecture. For information on specific agencies, customers, vendors, etc., concerning the System Security Plans (SSP) process, please reach out to the Application and Database Security Architect team.

Scope: These requirements apply to Network, Server and Database teams.

Requirements:

- 8.3 Information System Security Plans
  - Additional Notes:
    - If there is anything needed for Security purposes, it is most typically needed with respect to the Network Firewall Security Infrastructure, and is related to FSR's (Firewall Service Requests) that are needed to allow required network traffic between the Internet and hosted Web Servers, and/or the Edge Web Servers on the Agencies DMZ Networks communications to back end Database Servers or Applications Servers that are on the agencies Inside Private Networks.

    - Most of the SSP documents would probably be associated with the Web or Application Server configurations, with SQL or Oracle Database Servers configurations, Windows or Linux Server OS configurations, etc., that would be the responsibility of the appropriate Database Administrator or Server Support Team for those particular servers.
    - No input/resource from the Applications team.
    - Deskside - Refer to the Deskside Services team for related SOP.
- 8.5 Information Security Architecture
  - Additional Notes (SSP):
    - Project assignment and training on the gating process has changed scope and some planning as well as training and dissemination of resources needs to take place.
    - Security in Gating - Security Tasks
      - Intake
        - Work with customers to assess security risk using CA PPM.
        - Confirm risk level with CISO team if needed.
      - Initiate
        - Start to build security activities into project scope and schedule.
        - Review with customers and team.
      - Plan - Plan solution and Implementation
        - Detailed Design first
          - Review SSP and design with CISO. Create, update if needed.
          - Document into SSP what scans needed (from vendor or SecOps performed).
          - Request security scans.
      - Execute - Develop and deliver solution
      - Close - Transition solution to operations
      - After design and review - prepare security architecture deliverables.

Attachments/Folder:

- SP - Security Planning Cyber Pol 118
- Security architecture SOP
- Technical Standards - Design/Standard Documents
- Security in Gating
- CISP 017-Security Planning
- NIST SP 800-53 rev 4 (or as amended), Family
- Database Security Policy
- Security Tools SOP

Standard Operating Procedure

OIT Standard Operating Procedures Forms Index

Document Owner: OIT		Document ID:	
Technical Area: IAM, Server, Database, EA, SecOps, Network, SRC, Desktop/Deskside, OIS, CTO		Effective Date:	
Version: 0.2		Last Reviewed Date:	

Cyber Pol 111 - Media Protection

SOP Purpose: Standard operating procedure for identifying specific Governor's Office of Information Technology (OIT) requirements for Cyber Pol 111 Media Protection that details; Media Sanitization.

Scope: This requirement applies to the Data Center team.

Requirements:

- 8.5 Media Sanitation
    - Additional Note:
        - The Data Center does not have an SOP in place at this time. The SOP is a work in process, completion date TBD.

Attachments/Folder:

- MP - Media Protection Cyber Pol 111
- CISP 010: Media Protection
- NIST SP 800-53 rev 4 (or as amended), Family
- Electronic Media Reuse and Disposable

Revision History

Revision Date	Revised By	Brief Description of Changes	Approved By	Review Date
	Sherry Scott	Draft review, incorporated feedback	Chris H., Fatima B.	
	Sherry Scott	Draft review, incorporated feedback, added Scope	Chris H., Fatima B.	

Appendix